

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: John Favazza et al.
Serial No.: 10/626,208
Filing Date: July 24, 2003
Confirmation No.: 9671
Group Art Unit: 2137
Examiner: Shewaye Gelagay
Title: **SESSION TICKET AUTHENTICATION SCHEME**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicants respectfully request reconsideration of the application in light of the remarks set forth below.

REMARKS

Previously, Applicants received a Final Office Action dated April 9, 2008 (“*Office Action*”). At the time of the *Office Action*, Claims 1, 3, 5-8, and 24-36 were pending, of which, the Examiner rejected Claims 1, 3, 5-8, and 24-36 under 35 U.S.C. 103(a) as being unpatentable over US Publication No. 2003/0061512 to Flurry et al. (“*Flurry*”) in view of “Security Services Markup Language”, January 8, 2001 by Mishra (“*Mishra*”). Applicants contend that the rejections of Claims 1, 26, and 32 and each of their respective dependent claims contain clear legal and factual deficiencies as described below. Accordingly, Applicants request a finding that the rejections of Claims 1, 26, and 32 and each of their respective dependent claims are improper and that Claims 1, 26, and 32 and each of their respective dependent claims are allowable.

Claim 1 is directed to a method wherein a first request to grant a web service customer access to a first web service is intercepted at an agent residing between the web service customer and the first web service and between the web service customer and a second web service. One or more authentication credentials of the web service customer are collected at the agent, and it is determined at the agent whether the web service customer is authenticated and authorized. If the web service customer is authenticated and authorized, the first request is granted at the agent; the creation of a session and a session ticket is initiated at the agent; a session ticket ID for the session ticket is obtained at the agent; and **the session ticket ID and a public key are encrypted into an assertion at the agent**. In further accordance with the method, a second request to grant the web service customer access to the second web service is intercepted at the agent. **The second request comprises the assertion** and a signature associated with a private key. If the private key matches the public key in the assertion, the second request is granted at the agent without reauthenticating or reauthorizing the web service customer. Neither *Flurry* nor *Mishra*, alone or in combination disclose, teach, or suggest each of these limitations.

For instance, Claim 1 discloses that an agent “encrypt[s] [a] session ticket ID and a public key into an assertion.” Furthermore, the agent intercepts a second request for web service, “the second request comprising the assertion.” Thus, Claim 1 requires that the agent must receive the session ticket ID as part of the assertion included in the second request for web service.

The Examiner attempts to reject these limitations by relying on at least two different

tokens that are exchanged in the system of *Flurry*. However, as explained in more detail below, neither of these tokens disclose, teach, or suggest the limitations of Claim 1 as the Examiner argues. The first of these tokens contains a logon address rather than a session ticket ID while the second of these tokens is generated by the alleged agent of *Flurry* rather than being intercepted by the alleged agent of *Flurry* as would be required by Claim 1. Thus, neither of the tokens individually disclose, teach, or suggest “intercepting at the agent a second request to grant the web service customer access to the second web service, the second request comprising the assertion,” nor can the tokens be combined to do so.

The Examiner points to at least two different tokens in *Flurry* as the “session ticket ID” of Claim 1: the “aggregator token” of Paragraph [0073] and the “application authentication token” of Paragraph [0088]. *Office Action*, page 2, lines 15-18, and page 4, lines 16-20. The Examiner also identifies the ASP Aggregator of *Flurry* as the “Agent” of Claim 1. *Office Action*, page 4, line 11. Applicants do not necessarily agree with these identifications, but refer to them for the sake of argument.

Paragraph [0073] discloses that the aggregator token includes a logon address.

The **aggregator token comprises an address** that indicates the logon resource to which a user should be redirected if an ASP, aggregated application, or other entity in the ASP aggregator service's infrastructure determines that the user has not been properly authenticated when processing a request from the user for access to a resource that is supported or protected by the entity that received the request.

Flurry, paragraph [0073] (emphasis added). That is, the passage discloses that the aggregator token (the Examiner's first alleged Session ticket ID) comprises an address to which a user should be redirect to log on. Thus, *Flurry's* aggregator token does not disclose, teach, or suggest “a session ticket ID” as required by Claim 1.

Paragraph [0088] of *Flurry* discloses that the aggregator token (the Examiner's second alleged Session ticket ID) **is generated** by the ASP aggregator (the alleged Agent).

In contrast to the scenario described with respect to FIGS. 5A-5B, since the client/user has been previously authenticated by the ASP aggregator, the client/user would not receive an authentication challenge from the ASP aggregator. In other words, steps 538-546 in FIG. 5B would be unnecessary. Because the ASP aggregator has already authenticated the client/user, **the ASP aggregator would immediately generate the application authentication token** that is needed by the client/user with respect to the second aggregated application and then redirect the client/user to the second aggregated application. After the second aggregated application is received

and verified, the user may interact with the second aggregated application. Hence, in this scenario, the client's request to the second aggregated application undergoes two redirections, i.e. to and from the ASP aggregator and the second aggregated application, in a manner that should be transparent to the user.

Flurry, paragraph [0088] (emphasis added). That is, the passage discloses that the application authentication token (the Examiner's second alleged Session ticket ID) is generated by the ASP aggregator (the alleged Agent) **after** receiving the client's second request. Thus, *Flurry* does not disclose, teach, or suggest "intercepting at the agent" the session ticket ID as part of the second request as required by Claim 1.

In fact, the immediately preceding paragraph of *Flurry* makes it clear that subsequent requests for service in *Flurry* do not contain an application authentication token (the Examiner's second alleged session ticket ID) unless and until the application authentication token is generated by the ASP aggregator.

In this scenario, the user may have been authenticated by the ASP aggregator and may have interacted with a first aggregated application. At some later point in time, in a manner similar to that described above with respect to FIGS. 5A-5B, the user may attempt to interact directly with a second aggregated application using some type of saved session-specific information, e.g., a bookmarked URL that is associated with the second aggregated application. Since the user has attempted to interact directly with the aggregated application without the intermediate step of using the application workspace page, the second aggregated application **would not receive an application authentication token along with the client/user request.**

Flurry, paragraph [0087] (emphasis added). Accordingly, since the application authentication token of *Flurry* is generated by the ASP aggregator, it cannot be intercepted by the ASP Aggregator as part of the "assertion" as would be required by Claim 1.

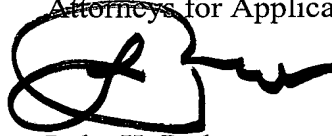
Consequently, at a minimum, *Flurry* fails to disclose, teach, or suggest the limitations, "intercepting at the agent a second request to grant the web service customer access to the second web service, the second request comprising the assertion" of independent Claim 1. For at least these reasons, independent Claim 1 and its dependent claims are allowable under 35 U.S.C. § 102. For analogous reasons, Applicants respectfully request that the rejections of independent Claims 26 and 32 and their respective dependent claims under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

As the rejections of Claims 1, 26, and 32 and each of their respective dependent claims contain clear legal and factual deficiencies, Applicants respectfully request a finding of allowance of 1, 26, and 32 and their respective dependent claims. If the PTO determines that an interview is appropriate, Applicants would appreciate the opportunity to participate in such an interview. To the extent necessary, the Commissioner is hereby authorized to charge any required fees or credit any overpayments to Deposit Account No. **02-0384** of **Baker Botts L.L.P.**

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants



Luke K. Pedersen
Reg. No. 45,003
214.953.6655

Date: 7-3-08

CORRESPONDENCE ADDRESS:

Customer No.: **05073**